1/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI

014624238 **Image available**
WPI Acc No: 2002-444942/200248
XRPX Acc No: N02-350535

Automatic valid IP configuration obtaining method in local area network, involves determining whether selected IP address from validated subset, is unused or not

Patent Assignee: FLUKE NETWORKS INC (FLUK-N)
Inventor: ARNDT M R
Number of Countries: 029 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
CA 2356067	A1	20020330	CA 2356067	A	20010829	200248	B
EP 1204260	A2	20020508	EP 2001308224	A	20010927	200248	
CN 1347227	A	20020501	CN 2001133059	A	20010912	200252	
JP 2002190811	A	20020705	JP 2001300447	A	20010928	200259	

Priority Applications (No Type Date): US 2000676631 A 20000930; US 2000237070 P 20000930
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
CA 2356067	A1	E	26	H04L-012/24	
EP 1204260	A2	E		H04L-029/12	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR					
CN 1347227	A			H04L-012/26	
JP 2002190811	A		9	H04L-012/28	

Abstract (Basic): CA 2356067 A1

NOVELTY - Network traffic is monitored and at least one subset in validated. An unused IP address in the subset is selected. The selected IP address is determined whether it is unused or not.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for valid IP configuration obtaining apparatus.

USE - For obtaining valid IP configuration automatically, in local area network and test instrument for networks.

ADVANTAGE - Provides improved network test instrument with valid IP configuration with corruption of other network hosts.

DESCRIPTION OF DRAWING(S) - The figure shows a perspective view of test instrument.

pp; 26 DwgNo 1/7

Title Terms: AUTOMATIC; VALID; IP; CONFIGURATION; OBTAIN; METHOD; LOCAL; AREA; NETWORK; DETERMINE; SELECT; IP; ADDRESS; VALID; SUBSET
Derwent Class: S01; T01; W01
International Patent Class (Main): H04L-012/24; H04L-012/26; H04L-012/28; H04L-029/12
International Patent Class (Additional): H04L-012/56
File Segment: EPI

1/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

07322324 **Image available**
DEVICE AND METHOD FOR AUTOMATICALLY ACQUIRING EFFECTIVE IP CONFIGURATION IN LOCAL AREA NETWORK

PUB. NO.: 2002-190811 A]
PUBLISHED: July 05, 2002 (20020705)
INVENTOR(s): ARNDT MANFRED R
APPLICANT(s): FLUKE NETWORKS INC

APPL. NO.: 2001-300447 [JP 2001300447]
FILED: September 28, 2001 (20010928)
PRIORITY: 00 676631 [US 2000676631], US (United States of America), September 30, 2000 (20000930)
00 237070 [US 2000237070], US (United States of America), September 30, 2000 (20000930)
INTL CLASS: H04L-012/28; H04L-012/56

ABSTRACT

PROBLEM TO BE SOLVED: To provide an enhanced device and method that can automatically acquire an effective IP(Internet Protocol) configuration without losing the performance of other network/host or the like.
SOLUTION: The device and method for automatically deciding the effective IP configuration on a network analyzes traffic and decides an effective sub-network, selects a start IP address that is not used in the sub-network with high probability and checks and discriminates whether or not the start IP address is available. When not available, the device and method decrements the value of the start IP address and again conducts the test until the effective address can be acquired.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－190811
（P2002－190811A）
(43)公開日　平成14年７月５日(2002.7.5)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）	
Ｈ０４Ｌ　12/28	２００	Ｈ０４Ｌ	12/28	２００Ａ	５Ｋ０３０
12/56			12/56	Ｂ	５Ｋ０３３

審査請求　未請求　請求項の数20　ＯＬ　（全９頁）

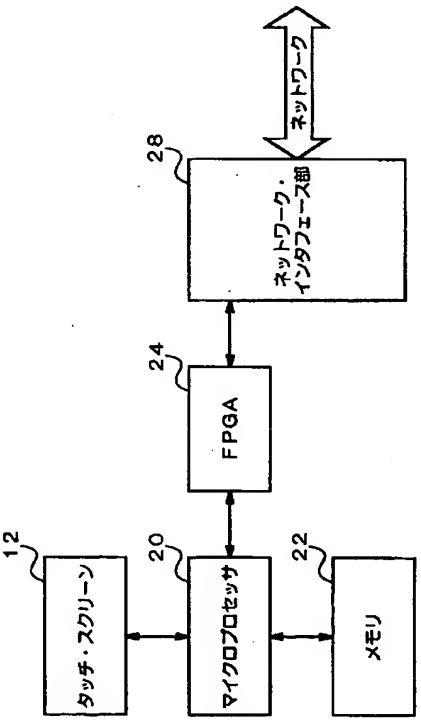
(21)出願番号　特願2001－300447(P2001－300447)
(22)出願日　平成13年９月28日(2001.9.28)
(31)優先権主張番号　０９／６７６６３１
(32)優先日　平成12年９月30日(2000.9.30)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　６０／２３７０７０
(32)優先日　平成12年９月30日(2000.9.30)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　501378826
フルーク　ネットワークス　インコーポレイテッド
Ｆｌｕｋｅ　Ｎｅｔｗｏｒｋｓ，　Ｉｎｃ．
アメリカ合衆国、ワシントン州98203、エベレット、シーウェイ　プールバード　6920
(74)代理人　100103171
弁理士　雨貝　正彦

最終頁に続く

(54)【発明の名称】　ローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する機器および方法

(57)【要約】
【課題】　他のネットワーク・ホストなどを損なうことなく有効なＩＰ構成を自動的に取得する、改善された機器および方法を提供すること。
【解決手段】　ネットワーク上の有効なＩＰ構成を自動的に決定する機器および方法は、トラフィックを分析し、有効なサブネットを決定する。サブネット内で未使用の可能性が高いスタートＩＰアドレスを選択し、検査して使用可能であるかどうか判断する。使用可能でない場合は、スタート・アドレスを減少させて、有効なアドレスが取得されるまで再びテストを行う。



1

【特許請求の範囲】

【請求項１】　ローカル・エリア・ネットワーク内で、有効なＩＰ構成を自動的に取得する方法であって、

ネットワーク・トラフィックを監視し、少なくとも１つのＩＰサブネットの妥当性検査を行う監視ステップと、

前記少なくとも１つのＩＰサブネット内で、未使用の可能性が高いＩＰアドレスを選択する選択ステップと、

選択されたＩＰアドレスが未使用であるかどうかを判断する判断ステップと、

を含むことを特徴とする方法。

【請求項２】　ネットワーク・トラフィックを監視して妥当性検査を行う前記監視ステップと、未使用の可能性が高いＩＰアドレスを選択する前記選択ステップの前に、ＤＨＣＰ（ダイナミック・ホスト・コンフィグレーション・プロトコル）を試行するＤＨＣＰ試行ステップと、

前記ＤＨＣＰを試行する前記ＤＨＣＰ実行ステップが成功した場合には、前記監視ステップおよび前記選択ステップを省略する省略ステップと、

をさらに含むことを特徴とするローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項３】　前記監視ステップは、ローカル・アドレスを識別することを特徴とする請求項１に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項４】　前記監視ステップは、前記ローカル・アドレスに対応するサブネット・マスクを識別することを特徴とする請求項３に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項５】　前記監視ステップは、ローカル・ルータを識別することを特徴とする請求項１に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項６】　前記監視ステップは、ローカル・サーバを識別することを特徴とする請求項１に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項７】　未使用の可能性が高いＩＰアドレスを選択する前記選択ステップは、ＩＣＭＰ（インターネット・コントロール・メッセージ・プロトコル）のアドレス・マスク要求を送信する要求送信ステップを含むことを特徴とする請求項１に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項８】　前記ＩＣＭＰのアドレス・マスク要求を送信する前記要求送信ステップがゼロのソースＩＰで実行されることを特徴とする請求項７に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項９】　発見されたローカル・ホストをアドレス範囲に配置するステップをさらに含むことを特徴とする請求項１に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

2

【請求項１０】　発見された前記ローカル・ホストがサブネット・マスクをレポートしたかどうかを判断し、レポートした場合には、前記ローカル・ホストのソースＩＰアドレスおよびサブネット・マスクを有するデータベース・アドレス範囲に前記ローカル・ホストを配置するステップをさらに含むことを特徴とする請求項９に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項１１】　発見された前記ローカル・ホストがサブネット・マスクをレポートしたかどうかを判断し、レポートしなかった場合には、前記ローカル・ホストのソースＩＰアドレスおよびサブネット・マスクを有するホストの数が最大であるデータベース・アドレス範囲に前記ローカル・ホストを配置するステップをさらに含むことを特徴とする請求項９に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項１２】　少なくとも１つのＩＰサブネット内で未使用の可能性が高いＩＰアドレスを選択する前記選択ステップが、最適なアドレス範囲を選択すること特徴とする請求項１に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項１３】　最も可能性が高いサブネット・マスクを選択するステップをさらに含むことを特徴とする請求項１２に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項１４】　最も可能性が高い前記サブネット・マスクが、トラフィック分析の結果発見されたマスクを含むことを特徴とする請求項１３に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項１５】　最も可能性が高い前記サブネット・マスクが、ユーザによって最後に指定されたマスクを含むことを特徴とする請求項１３に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項１６】　最も可能性が高い前記サブネット・マスクが狭いマスクとして選択され、選択されたアドレス範囲内のすべてのローカル・アドレスが実質的に前記サブネット・マスク内に収まるまで、または限界に達するまで、前記マスクが拡大されることを特徴とする請求項１３に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項１７】　ソースＩＰスタート値がＩＰチェック・アドレス値として選択され、かつＩＰアドレスが未使用かどうかを判断する前記判断ステップが前記ＩＰチェック・アドレス値を使用して実行されることを特徴とする請求項１２に記載のローカル・エリア・ネットワーク

内で有効なＩＰ構成を自動的に取得する方法。

【請求項１８】　前記ＩＰチェック・アドレスが使用できない場合は、使用可能なアドレスが決定するまで前記ＩＰチェック・アドレスを繰り返し変更することを特徴とする請求項１７に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法。

【請求項１９】　ローカル・エリア・ネットワーク内で、有効なＩＰ構成を自動的に取得する機器であって、少なくとも１つのＩＰサブネットの監視および妥当性検査を行うためのネットワーク・トラフィック・モニタと、

少なくとも１つのＩＰサブネット内で未使用の可能性が高いＩＰアドレスを選択し、かつ選択されたＩＰアドレスが未使用であるかどうかを判断するためのＩＰアドレス・セレクタと、

を備えることを特徴とする機器。

【請求項２０】　前記ＩＰアドレス・セレクタは、ソースＩＰスタート値をＩＰチェック・アドレス値として選択し、前記ＩＰアドレスが未使用かどうかの判断を前記ＩＰチェック・アドレス値を使用して行うことを特徴とする請求項１９に記載のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークに関し、さらに詳細には、ＬＡＮ内およびネットワークのテスト機器内で、有効なＩＰ構成を自動的に取得する機器および方法に関する。

【０００２】

【従来の技術】交換ネットワーク構成では、ネットワークに接続されている装置のＩＰアドレスを取得する方法、およびネットワーク上の装置のＩＰアドレスの有効性を確認する方法に関して問題が生じる。交換環境では、ポートは、通過する限られたトラフィックを見るだけであり（一般にそのポートに向けて送られるトラフィックのみ）、監視可能なデータの量は限られる。あるいは、装置が接続されているポートでブロードキャスト・トラフィックのみが見えることも多い。

【０００３】装置は、ネットワーク上で動作する際に使用する有効なＩＰアドレスを選択したいと希望する。ところが現代のネットワークでは、不正確なサブネット・マスクと構成の誤ったＩＰアドレスの発生が後を絶たないため、ネットワーク・トラフィックを監視することにより、衝突する結果や重なり合う結果を得ることがあり、そのため正しいローカル・アドレスの範囲を識別するのが困難なことがある。ネットワーク上ですでに別の装置が使用しているアドレスをその装置がたまたま選択した場合、そのＩＰアドレスが偶然選択されたことによって別のネットワーク装置が自分のアドレス・キャッシュを不正に更新することになり、そのＩＰアドレスの本

来の有効な所有者に向けたトラフィックが失われたり、誤送信されたりすることがある。これは非常に望ましくないが、それ自体がネットワーク上で問題を引き起こしてはならないテスト機器では特に望ましくない。

【０００４】さらに、装置による適切なサブネット・マスクおよびデフォルト・ルータの選択が不可欠である。というのは、マスクとルータが正しくないと、装置がネットワーク上の他の装置と適切に通信できないためである。適切なドメイン・ネーム・サーバ（ＤＮＳ）の選択もまた重要である。ドメイン・ネーム・サーバは、暗号めいたＩＰアドレスよりもユーザが覚えやすい、象徴的な名前に対応するＩＰアドレスを返す。ＤＮＳが不適切に選択されると、特定の名前に関連付けられたＩＰアドレスをそのＤＮＳが知得していない場合には名前解決が行われない。装置は、不適切に選択されたＤＮＳと通信することさえできない場合がある。

【０００５】ある特定のネットワークが、ＩＰアドレスの範囲（たとえば、Ａ．Ｂ．Ｃ．６４からＡ．Ｂ．Ｃ．１２７）を取得するためのマスク値でＩＰアドレスをマスクしたサブネット・マスクを使用していることもある。このサブネットの有効なＩＰアドレスは、アドレスの最後の部分が６４から１２７の範囲になっている。テスト機器（またはその他の装置）がこの範囲内のＩＰアドレスを使用していない場合には（たとえば、６４から１２７の範囲外となるＡ．Ｂ．Ｃ．２５０）、ネットワーク上の他の装置からの応答が戻ってこない。というのは、他の装置が、このＩＰアドレス（この例ではＡ．Ｂ．Ｃ．２５０）があるはずのネットワークに転送するためにいつまでもルータへパケットを送るため、データがこの装置に受け取られないためである。

【０００６】従来は、連続した１つの範囲のＩＰアドレスが所定ののネットワークで使用されると、この範囲外のＩＰアドレスはルータを通らざるを得なかった。しかし現在では、数多くの不連続のＩＰアドレス範囲が同じネットワーク・ケーブル上にあるのが普通である。どの範囲が有効であるかを判断するのは困難な場合がある。

【０００７】従来の試験装置は、ユーザがその装置の使用するＩＰアドレスを供給することを必要とし、一定水準のネットワークの知識を要し、無効なＩＰアドレスで不適切に構成された装置がないということを前提としていた。ＩＰアドレスが重複した装置が２つ以上あると、断続的にネットワーク問題が発生することがある。たとえば、イーサネット（登録商標）では、ＩＰアドレスはハードウェア・アドレスによって解決される（ＭＡＣ（メディア・アクセス・コントローラ）のアドレス）。個々の装置はＭＡＣアドレス（一般に４８ビット）のＡＲＰキャッシュ（アドレス解決プロトコル）を維持し、ネットワークがアクセスされるたびにＡＲＰを行わなくても済むようにする。ネットワーク上の２つ以上のホストが使用しているＩＰアドレスについてＡＲＰを行う

と、複数の応答があり、ネットワーク上で他のホストのＡＲＰキャッシュが不確定に更新される。そのため、ＡＲＰキャッシュ内のＭＡＣアドレスは頻繁に変化しているので、重複するＩＰアドレスに送信されるフレームは、その時点の誤った装置部分へ向かう。次いで、ホストは時折、ＩＰアドレスのＭＡＣアドレスへのマッピングがＩＰアドレスの「望ましい所有者」を示すようにＡＲＰキャッシュを更新する。この時点では、ＡＲＰキャッシュの更新によって送信が適切な装置に向かう。そのため、（ユーザには）容易にわからない理由で、通信が偶然に再び機能し始める。テスト機器はネットワークを損なってはならないため、このような状況は、可能なら回避するべきである。

【０００８】

【発明が解決しようとする課題】本発明、すなわち構成がＤＨＣＰ（ダイナミック・ホスト・コンフィグレーション・プロトコル）によって取得できない場合にＩＰ構成を自動的に取得する方法によれば、トラフィックが連続的に監視されて、サブネット・マスク、ローカル・ルータおよびサーバに対応するローカル・アドレスを識別する。収集された情報はデータベースに格納され、ある時間後、有効なＩＰサブネットと無効なＩＰサブネットが決定される。

【０００９】したがって、本発明の目的は、他のネットワーク・ホストなどを損なうことなく有効なＩＰ構成を自動的に取得する、改善されたネットワークテスト機器を提供することである。さらに本発明の目的は、可搬ネットワーク装置の有効なＩＰ構成を自動的に取得する、改善された方法を提供することである。

【００１０】

【課題を解決するための手段】上述した課題を解決するために、本発明のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する方法は、ネットワーク・トラフィックを監視し、少なくとも１つのＩＰサブネットの妥当性検査を行う監視ステップと、少なくとも１つのＩＰサブネット内で、未使用の可能性が高いＩＰアドレスを選択する選択ステップと、選択されたＩＰアドレスが未使用であるかどうかを判断する判断ステップとを含んでいる。

【００１１】また、本発明のローカル・エリア・ネットワーク内で有効なＩＰ構成を自動的に取得する機器は、少なくとも１つのＩＰサブネットの監視および妥当性検査を行うためのネットワーク・トラフィック・モニタと、少なくとも１つのＩＰサブネット内で未使用の可能性が高いＩＰアドレスを選択し、かつ選択されたＩＰアドレスが未使用であるかどうかを判断するためのＩＰアドレス・セレクタとを備えている。

【００１２】本発明の主題は、本明細書の末尾で具体的に指摘され、明確に特許請求されている。しかし、編成と動作方法、ならびに他の利点および目的は、以下の説明を添付の図面と併せ読めば、よりよく理解できよう。図面では、同じ参照記号は同じ要素を指す。

【００１３】

【発明の実施の形態】本発明の好ましい一実施形態によるシステムは、有効なＩＰ構成を自動的に取得可能なネットワーク分析機器および方法を具備する。図１は、本発明を実施した代表的なネットワークテスト機器の斜視図である。図１に示すテスト機器１０は、ネットワークの試験および分析用の可搬機器として適切に構成されている。ディスプレイ１２は、ユーザとテスト機器１０との間の対話を可能にする。ディスプレイは適切にはタッチ・スクリーン型ディスプレイであり、スタイラス１４は、ユーザがテスト機器１０との対話で使用することができる。ケースの上部に沿って様々なステータス・インジケータ１６が設けられ、リンク状況、送信、衝突、エラー、利用率などを示す。電源ボタン１８も設けられている。このテスト機器１０は、内部のバッテリ・システムによって給電するのが適切であるが、外部の電源に接続することもできる。このテスト機器１０は、ネットワーク・トラフィック・モニタとしての機能と、ＩＰアドレス・セレクタとしての機能を備えている。

【００１４】図２は、本テスト機器１０の高水準のブロック図である。マイクロプロセッサ２０は、情報の表示および受取りを行うタッチ・スクリーン１２と接続されている。メモリ２２は、マイクロプロセッサ２０に接続されている。ＦＰＧＡ（Field Programmable Gate Array）２４もマイクロプロセッサ２０に接続されている。ネットワーク・インタフェース部２８は、ネットワークとの実際の送信および受信の詳細を処理する。

【００１５】図３、図４、図５は、本発明を適用したテスト機器１０が実行するステップの流れ図である。図３に示すように、テスト機器１０がネットワークに接続されている場合に、初めにテスト機器１０はネットワーク・トラフィックの監視を開始する（ステップ１００）。以下にさらに詳しく説明するように、テスト機器１０は、継続してトラフィックを監視し、受信した情報の識別およびデータベースへの格納を行う。

【００１６】ステップ１００の監視が行われている間と継続して行われる間、監視と並行して、リンクが検出され次第ＤＨＣＰ（ダイナミック・ホスト・コンフィグレーション・プロトコル）が試行され、ＩＰアドレスの取得が試みられる（ステップ１０２）。当技術分野で周知のとおり、これはメッセージをブロードキャストしてＤＨＣＰサーバを捜し出すことを含む。この試行が成功した場合は（判断ステップ１０４）、ＤＨＣＰサーバがＩＰアドレス、サブネット・マスク、デフォルト・ルータ、ＤＮＳサーバ、およびＩＰアドレスの有効期間をもって応答し、ＩＰ構成を取得するプロセスは終了する。

【００１７】ところが、多数のネットワークにＤＨＣＰサーバが存在しないことや、サーバが一時的に使用でき

ないことがあるが、これはネットワーク技術者が解決を試みているネットワーク動作問題、したがってテスト機器の使用に起因している可能性がある。従来の技術によれば、ＤＨＣＰが成功しなかった場合、従来の装置はＤＨＣＰを試行し続けるので、ＤＨＣＰが成功するまで、あるいはユーザが手動で有効なＩＰ構成を与える（これは接続しているネットワークについてユーザがあらかじめ知識を有していない場合は非常に困難である）まで先へ進めない。

【００１８】本明細書で述べるテスト機器、装置、または方法によれば、ＤＨＣＰが成功しなかった場合は、ゼロのソースＩＰ（０．０．０．０）のままインターネット・コントロール・メッセージ・プロトコル（ＩＣＭＰ）のアドレス・マスク要求が送信される（ステップ１０５）。ＩＣＭＰは、例えば、ルータが他のホストへＩＰ構成情報を通知できることを含めて、数多くのことを行うプロトコルである。ＩＣＭＰアドレス・マスク要求は、ゼロのソースＩＰ（０．０．０．０）に回答できるように定義された数種のＩＰパケットの１つである。ソースＩＰがゼロであると、大部分のＩＰパケットはＴＣＰ／ＩＰスタックによって破棄される。ＩＣＭＰ要求に応答して、２５５．２５５．２５５．２５５へブロードキャストして回答を返すものがあるため、対応するサブネット・マスクを有するホストのアドレスもさらにわかる。一部のルーティング・プロトコル（たとえば、ＯＳＰＦおよびＲＩＰ２）は、サブネット・マスクを公表する。

【００１９】システムは、ネットワーク上のトラフィックを継続して監視し、トラフィックから、およびＩＣＭＰ要求に対して生成された応答から情報を収集する。ステップ１００の監視によってローカル・ホストが発見された時点でステップ１０６が実行され、ネットワーク上で発見されたホストをアドレス範囲内に配置する。ホストとは、ネットワーク上でアドレス可能な装置に与えられた名前である。接続されているネットワークにとってローカルでないＩＰアドレスは、識別されて破棄される（例えば、大部分のルーティング・プロトコルおよびＡＲＰ要求は、ローカル・ホストからのものである）。

【００２０】判断ステップ１０８では、発見されたホストがサブネット・マスクをレポートしたかどうか判断する。ホストがレポートした場合には、そのホストのソースＩＰアドレス、およびそのホストと同じサブネット・マスクを含んだアドレス範囲のデータベース内にホストが配置される（ステップ１１０）。判断ステップ１０８の結果、発見されたホストがサブネット・マスクをレポートしなかった場合には、この特定のホストは、このホストのソースＩＰを含んでいて、一致するサブネット・マスクを示すホスト数が最大であるアドレス範囲内に配置される（ステップ１１２）。ステップ１１０または１１２の後で、十分な監視時間が経過したかどうか判断し（ステップ１１４）、経過していない場合は、追加のホストが発見されると、ステップ１０６の処理に進む。監視時間は変わることがあるが、例として一般に約２０秒を含むことができる。時間は予め決定しておいてもよいが、ネットワーク・トラフィックに基づく使用可能なデータ量に応じて変化してもよい。所定の時間内のトラフィックが少ないということは、さらに確固としたデータ・セットが得られるように、監視の時間を長くすることを示唆していると考えられる。時間が終了した後は、妥当性検査処理を実行して、有効および無効のアドレス範囲を決定する（ステップ１１６）。この処理は、重なり合ったアドレス範囲の検査、有効および無効のＩＰサブネットの決定を含む。この決定は、特定のサブネット・マスクを示すホストの数に基づいた最適な合意を使用して行う。次のステップ１１８では、無効な範囲内に配置されているホストが、適切な妥当性ある範囲に移動される。

【００２１】次に、図４に示すように、ある時間後に（ステップ１２２）、収集したトラフィック情報を使用して、ローカル・セグメント上の最適なアドレス範囲が選択される。「最適な」アドレス範囲を選択するためには、サブネット・マスクが発見されたサブネット、またはルータが見つかったサブネットが好ましい。優先順位の階層で次にくるのは、大多数のホストを含むＩＰサブネットを使用することである。このローカル・アドレス範囲が選択された後は、ステップ１２４が実行され、最も可能性が高いサブネット・マスクが選択される。このサブネット・マスクは、テスト機器のソースＩＰを選択するためにのみ使用され、実際には使用されないこともある（例えば、後からさらに適したものが見つかった場合）。サブネット・マスクを選択するためには、トラフィック分析の結果サブネット・マスクが発見された場合は、その発見されたサブネット・マスクが使用される。発見されなかった場合は、最後にユーザ指定されたサブネット・マスクが現在のネットワークで有効であることが明らかであれば、それが使用される。最後の手動構成は全体が保存され、望むなら使用することができる。そうでない場合は、非常に狭いサブネット・マスクを試み、選択された最適なアドレス範囲内のローカル・アドレスがすべてサブネット・マスク内に収まるまで、または２５５．２５５．２５５．０に達するまで拡大する。例えば、２５５．２５５．２５５．２４８という最初のサブネット・マスクを試みることができる。これがうまくゆかない場合、つまり選択された最適なアドレス範囲内にある、監視中に発見されたローカル・アドレス全部がそのマスク内に収まりきらない場合は、マスク内で別の最下位ビットが許可され、例えば２５５．２５５．２５５．２４０になる。このマスクと後続のマスクが適切でない場合は、次々にマスクを２５５．２５５．２５５．２２４、２５５．２５５．２５５．１９２、および

２５５．２５５．２５５．１２８として試みる。最後にマスクが２５５．２５５．２５５．０に達した場合は、これがサブネット・マスクとして使用されて、テスト機器（またはその他の装置）のソースＩＰの選択が行われる。

【００２２】次のステップ１２６では、テスト機器１０がソースＩＰを見つけようと試行する。初めにＩＰがスタート・オクテット値を使用して設定され、この値はユーザが特定の値に事前選択してもよいが、テスト機器１０のユーザが選択しない場合は、２５０を適当なデフォルトとするスタート値になる。したがって、特定の「最適な」ＩＰアドレス範囲Ａ．Ｂ．Ｃ．ＸＸＸが与えられると、スタート・オクテット値がＸＸＸに置き換えられ、サブネット・マスクはＡ．Ｂ．Ｃ．ＸＸＸの値に割り当てられる。次に、発見データベース（テスト機器１０によってこの特定のネットワーク上で観取または「発見」されたＩＰアドレスおよびその他の情報のデータベース）を検査して（判断ステップ１２８）、そのソースＩＰがネットワーク上で活性であるかどうかを調べる。Ａ、Ｂ、およびＣはＩＰアドレス値を示し、装置が接続されているネットワークに応じて決まる。たとえば、特定のネットワークのＡ．Ｂ．Ｃが２６０．８３．１０であり、サブネットが．１２８から．１９１の範囲である場合、機器は２６０．８３．１０．１２８を取り、そのマスクに割り当てられたスタート・オクテットの２５０（デフォルト・スタート・オクテットの２５０およびサブネット・マスク２５５．２５５．２５５．１９２を仮定）を加えて、アドレス２６０．８３．１０．１８６が得られる。機器は、初めに発見データベースでアドレスを捜すことにより、２６０．８３．１０．１８６がすでに確かめられているかどうかを検査して調べる。その特定のソースＩＰが活性である場合は、ステップ１３０でソースＩＰを減少させ（２６０．８３．１０．１８５になる）、判断ステップ１２８へ戻って、すでに発見データベースにこのＩＰがあるかどうか調べる。活性なソースＩＰでなく、かつソースＩＰが有効なサブネット範囲内（この例では．１２８から．１９１）にある値が決まるまで、減少と検査を繰り返して処理を行う。

【００２３】次に、処理が続行されて、例えば「無償ＡＲＰ」によって、ソースＩＰがすでに使用されているかどうかを検査する。検査は、任意選択で米国特許第５，７２４，５１０号に記載されている方法によって行うこともでき（ステップ１３２）、この特許の開示を参照により本明細書の一部とする。ホストは一般にＡＲＰキャッシュを維持し、これがネットワーク上の他のホストの４８ビット・メディア・アクセス・コントロール・アドレス（ＭＡＣアドレス）を格納する。しかし、所望の目標はＡＲＰキャッシュの破損（すでに使用されているＩＰアドレスを「無償ＡＲＰ」で試験した場合に発生することがある）を回避し、管理者コンソールでのコンソール・エラー・メッセージの生成またはログ・ファイル・エラーの生成を回避することなので、任意選択のステップを使用することにより追加のダブル・チェックが実現する。ソースＩＰが別のホストに使用されている場合は（判断ステップ１３４）、ステップ１３０で処理が続行され、ＸＸＸ領域がさらに減分されて別のソースＩＰが試行される。すでに発見されているＩＰアドレスの発見データベースに照らしてソースＩＰを検査すると、ＩＰアドレスを自動で見つける処理の速度が上がり、ネットワーク要求を生成して可用性の検査を試行することに起因する不必要なネットワーク・トラフィックが減少する。

【００２４】一方、判断ステップ１３４でソースＩＰが使用されていないと判断された場合は、処理が図５に示すステップに進む。図５に示すように、この場合は（有効なソースＩＰがあるため）ＴＣＰ／ＩＰスタックが応答するので、ローカルのＩＰ構成を識別するための追加の発見要求がネットワーク上に送信される。これらの要求は、例えば、ネットワーク構成とその上のホストに関する情報をさらに取得するための、ＩＣＭＰルータ要請（Router Solicitation）、およびＩＣＭＰアドレス・マスク、ＩＣＭＰエコー、ＳＮＭＰマスク要求およびＤＮＳ発見要求（Discovery Request）を含む。これらの要求は、全ローカル・ホストからの応答を迅速に要求するため、限られたＩＰブロードキャスト・アドレスである２５５．２５５．２５５．２５５に送信される。

【００２５】これらの追加の発見要求が処理された後で、テスト機器１０は、発見された最適なデフォルト・ルータ、最適なサブネット・マスク、および最適なＤＮＳサーバを選択する（ステップ１３８）。最適なデフォルト・ルータを決定するため、テスト機器と同じアドレス範囲にあるすべてのルータＩＰアドレスが比較される。好ましいルータは、使用するルーティング・プロトコルに基づいて選択される。例えば、好ましい実施形態では、ＯＳＰＦ（Open Shortest Path First）プロトコルに高いランクが与えられ、ＥＩＧＲＰ（Enhanced Interior GatewayRouting Protocol）などがこれに続く。階層上で下位にあるその他のプロトコルは、ＲＩＰ（Routing Information Protocol）およびＩＲＤＰ（ＩＣＭＰ Router Discovery Protocol）である。階層内でルーティング・プロトコル優先順位が同じであるＩＰアドレスが複数見つかった場合は、下位のＩＰアドレスが選択される。選択されるＤＮＳサーバは、テスト機器と同じアドレス範囲にある最も下位のＤＮＳサーバＩＰアドレスである。しかし、テスト機器１０と同じアドレス範囲でＤＮＳサーバが見つからない場合は、何らかの発見されたＤＮＳサーバが選択される。ＤＮＳサーバが発見されなかった場合は、最後にユーザ指定された構成からＤＮＳサーバが使用される。

【００２６】テスト機器１０またはその他の装置が自動

ＩＰ構成処理を終了した後は、周期タイマをスタートして、時折、構成の妥当性検査および自動修正を行うことができる。これは、完全自動構成を使用した場合に限って使用するのが適当である。構成を手動で設定した場合や部分的にユーザが補助した場合は、自動修正を省略することが好ましい。周期タイマは、好ましい実施形態では５秒が適当であり、長い時間、たとえば５分が経過した後で、自動修正処理を停止できるのが適当である。

【００２７】次に、テスト機器１０は、前述の自動修正ステップと平行してセグメント発見試験を自動実行し、ブロードキャスト・ドメイン内（同じブロードキャストを受信するネットワークのうちの一部）にある全ネットワーク装置を分析して、ローカル・ホスト、スイッチ、ルータ、サーバ、およびその他のネットワーク装置を検出することができる。したがって、ＩＰアドレス、ＭＡＣアドレス、サブネット・マスクなどの他のアドレッシング情報も適当に発見される。一部の装置がブロードキャストに応答しないこともあるため、これはユニキャスト・トラフィックで実施するのが適当である。様々な装置およびネットワークの詳細なデータベースが編纂される。自動修正処理は、さらに適したルータ、ＤＮＳサーバ、または適切なサブネット・マスクが識別された場合に、データベースを使用してＩＰ構成を更新する。

【００２８】図６は、特定の状況での妥当性検査の例、すなわち対応するサブネット・マスクを有するアドレス範囲からなる非連続なグループが複数見られるアドレス範囲およびホスト位置を示すグラフに示す。図６では、多数の有効なホストがアドレス範囲５０にある。加えて、多少のホストがアドレス範囲５２と５４にある一方、それよりもかなり多くのホストがアドレス範囲５６にある（それでも範囲５０のホストの数よりは少ない）。図６に示す状況では、すべてのアドレス範囲の妥当性検査が行われ、領域５０内のアドレス範囲が「最適な」アドレス範囲として選択される。

【００２９】図７は、別の可能な状況での妥当性検査を示すグラフである。この構成では、大きなアドレス範囲６０内に完全に含まれているアドレス範囲５８の境界内に、多数のホストからなるグループが含まれている。この構成では、アドレス範囲５８内のホストの妥当性検査が行われ、他方、範囲６２および６４内のホストは、衝突情報であるため妥当性検査が行われないまま残される。

【００３０】妥当性検査処理では、初めにホストは、属することをホストが示した所に配置される。妥当性検査後にホストは、それが収まる最初に妥当とされたアドレス範囲内に置かれる。ホストが収まる有効なアドレス範囲がない場合は、ホストがサブネット・マスクを有していれば、ホストが配置を要すると示した所に置かれ、あるいはそのホストが収まる大部分のホストがあるアドレス範囲内に置かれる。

【００３１】以上、本発明によれば、有効なＩＰ構成を自動的に取得する機器および方法を示し説明してきた。これによりテスト機器は、ネットワーク上でネットワーク問題を引き起こすことなく、ＩＰアドレスを取得することができる。例示した実施形態について、主にネットワークテスト機器の場合について説明したが、本発明は、適切にはネットワークに接続できるその他の装置がＩＰ構成を自動的に取得するためにも適用される。たとえば、本発明の方法または機器を使用した可搬コンピュータ（ラップ・トップ型、ノート型など）は、これを都合よくネットワークに接続して、ＩＰ構成を自動的に取得できる。

【００３２】本発明の好ましい一実施形態を示し説明してきたが、本発明の幅広い態様から逸脱することなく、本発明に数多くの変更および修正を加えることができることは、当業者には明らかであろう。したがって、付記した特許請求の範囲は、本発明の真の精神および範囲内に入るこのような変更および修正をすべて包含するものとする。

【図面の簡単な説明】

【図１】有効なＩＰ構成を自動的に取得する本発明の方法を適用したテスト機器の斜視図である。

【図２】本発明を適用したテスト機器の高水準ブロック図である。

【図３】ＩＰ構成を取得するステップの流れ図である。

【図４】ＩＰ構成を取得する他のステップの流れ図である。

【図５】ＩＰ構成を取得する他のステップの流れ図である。

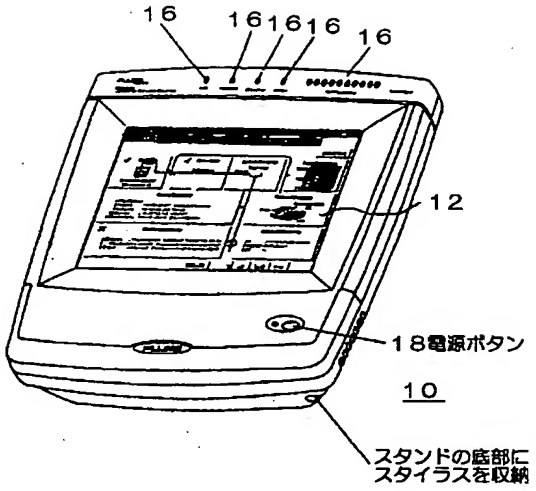
【図６】可能な一状況でのアドレス範囲の妥当性検査および「最適な」アドレス範囲の選択を示すグラフである。

【図７】別の可能な状況でのアドレス範囲の妥当性検査を示すグラフである。

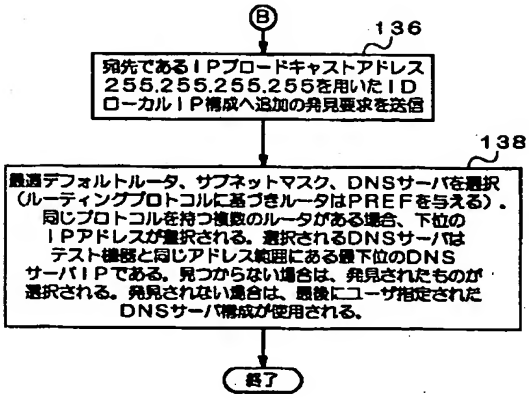
【符号の説明】

１０　ネットワーク機器
１２　タッチ・スクリーン
１４　スタイラス
１６　ステータス・インジケータ
１８　電源ボタン
２０　マイクロプロセッサ
２２　メモリ
２４　ゲート・アレイ
２８　ネットワーク・インタフェース部

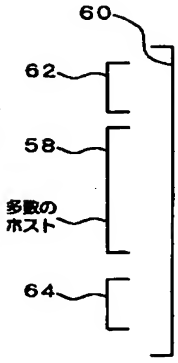
【図１】


16
16
16
16
16
12
１８電源ボタン
10
スタンドの底部に
スタイラスを収納
１４スタイラス

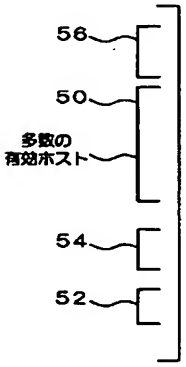
【図５】


Ⓑ
136
宛先であるＩＰブロードキャストアドレス
255.255.255.255を用いたＩＤ
ローカルＩＰ構成へ追加の発見要求を送信
138
最適デフォルトルータ、サブネットマスク、DNSサーバを選択
（ルーティングプロトコルに基づきルータはＰＲＥＦを与える）。
同じプロトコルを持つ複数のルータがある場合、下位の
ＩＰアドレスが選択される。選択されるDNSサーバは
テスト機器と同じアドレス範囲にある最下位のDNS
サーバＩＰである。見つからない場合は、発見されたものが
選択される。発見されない場合は、最後にユーザ指定された
DNSサーバ構成が使用される。
終了

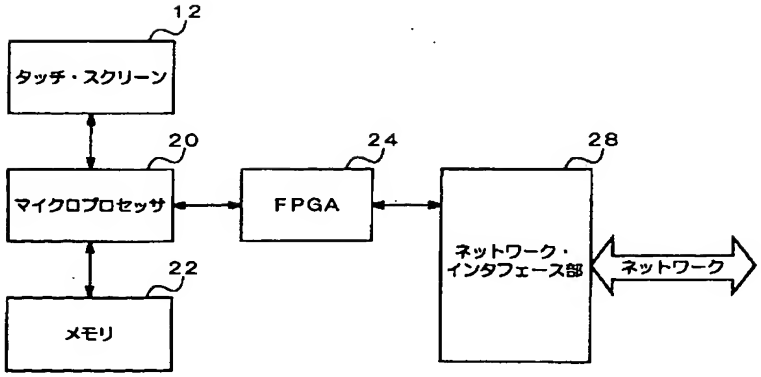
【図７】


60
62
58
多数の
ホスト
64

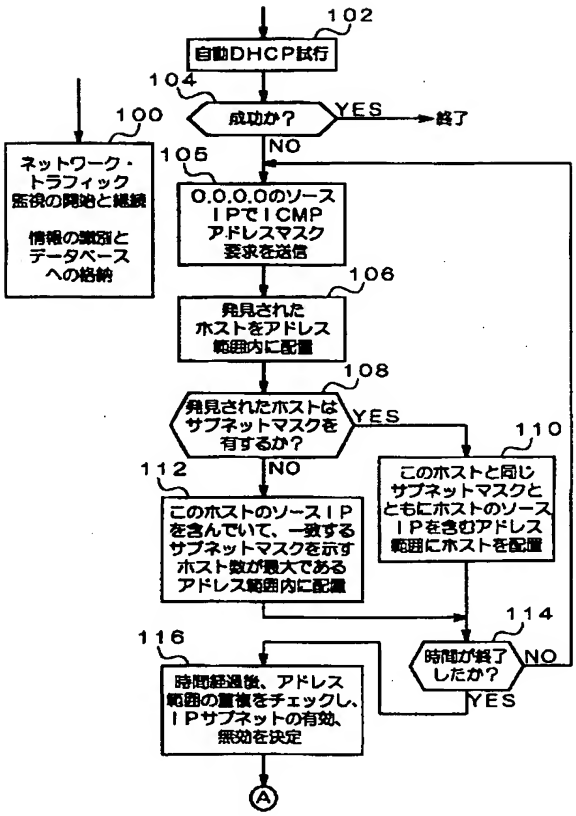
【図６】


56
50
多数の
有効ホスト
54
52

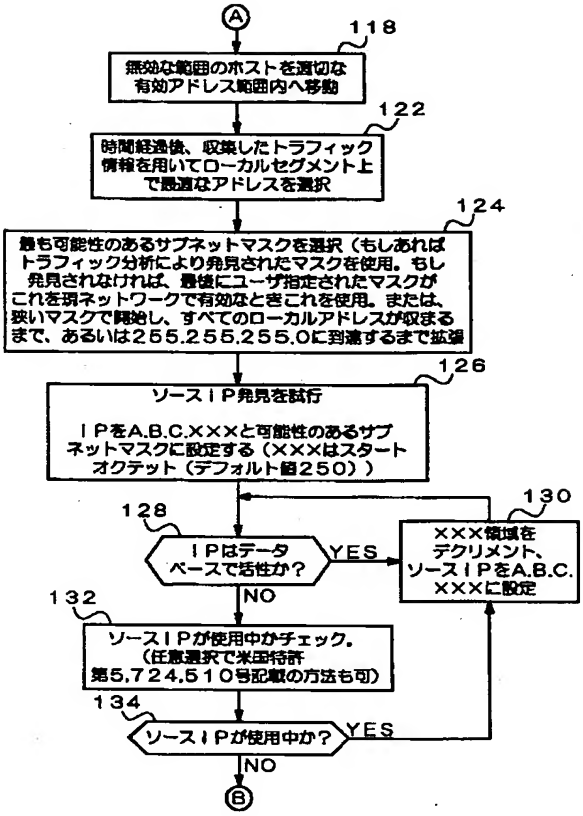
【図２】


12
タッチ・スクリーン
20
マイクロプロセッサ
24
FPGA
28
ネットワーク・
インタフェース部
ネットワーク
22
メモリ

【図３】



【図４】



フロントページの続き

(71)出願人　501378826
6920　Seaway　Boulevard
Everett,　Washington　98203　US

(72)発明者　マンフレッド　R　アンツ
アメリカ合衆国、コロラド州80919、コロラドスプリングス、コーポレートドライブ　6805　100号室　フルーク　ネットワークス　インコーポレイテッド内

Fターム(参考)　5K030 HC14 HD09 JA10 JT09 MB09
5K033 AA03 CC01 DB20 EA07 EC03